Tarek H. Zohdy (SBN 247775)
Tarek.Zohdy@capstonelawyers.com
Cody R. Padgett (SBN 275553)
Cody.Padgett@capstonelawyers.com
Trisha K. Monesi (SBN 303512)
Trisha.Monesi@capstonelawyers.com
Capstone Law APC
1875 Century Park East, Suite 1000
Los Angeles, California 90067
Telephone: (310) 556-4811
Facsimile: (310) 943-0396

Attorneys for Plaintiffs
Cynthia Husebo and Matthew Tidd

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

CYNTHIA HUSEBO and MATTHEW TIDD, individually, and on behalf of a class of similarly situated individuals,

Plaintiffs,

v.

MARRIOTT INTERNATIONAL, INC., a Delaware corporation, and MARRIOTT HOTEL SERVICES, INC., a Delaware corporation,

Defendants.

Case No.:

CLASS ACTION COMPLAINT FOR:

(1) Violations of Unfair Competition Law, California Business & Professions Code § 17200 *et seq.*
(2) Violations of California's Customer Records Act, California Civil Code § 1798.80 *et seq.*
(3) Negligence
(4) Deceit by Concealment

DEMAND FOR JURY TRIAL

INTRODUCTION

1. Plaintiffs Cynthia Husebo and Matthew Tidd ("Plaintiffs") bring this action for themselves and on behalf of all persons who reside in the United States and who made a reservation at a hotel, or substantially similar property, owned and/or managed by Marriott International, Inc. or Marriott Hotel Services, Inc. ("Defendants" or "Marriott"), from four years prior to the filing of this complaint to the time of class certification, whose personal or financial information was accessed, compromised, or stolen as a result of the 2014 Data Breach ("Marriott Guests").

2. Marriott requires its Guests to provide personally identifiable information ("PII") upon making a reservation via Defendant's website, reservation phone line, or mobile phone application, and Marriott Guests expect Defendants to maintain strict confidentiality of their PII in Marriott's possession. Throughout the course of its business, Marriott has collected and maintained an extensive amount of its Guests' personal information including, without limitation, names, email addresses, home and billing addresses, telephone numbers, dates of birth, credit card numbers, passport numbers, and reservation history. However, on information and belief, Defendant failed and continues to fail to protect adequately its Guests' personal and confidential information. Furthermore, Defendant has egregiously failed to provide sufficient and timely notice or warning of potential and actual cybersecurity breaches to its Guests.

3. In an ongoing investigation, Marriott recently revealed that its Guests' personal information was subject to a massive data security breach "since 2014" and "believes [the unauthorized accessed data] contains information on up to approximately 500 million guests who made a reservation at a Starwood property" ("2014 Data Breach").[1] Remarkably, Marriott waited

[1] "Starwood Guest Reservation Database Security Incident," available at https://answers.kroll.com/ (last visited December 3, 2018).

until November 30, 2018, to publicly inform its Guests of the 2014 Data Breach for the first time. According to the statement, "[o]n September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database."[2] Further, "[f]or approximately 327 million of these guests, the information [stolen] includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates." To date, Marriott states that it "began sending emails on a rolling basis … to affected guests whose email addresses are in the Starwood guest reservation database," but no other actions have been taken.

4. As a result of Defendant's failure to maintain adequate security measures and timely security breach notifications, Marriott Guests' personal and private information has been compromised and remains vulnerable. In fact, according to Marriott, they have "not finished identifying duplicate information in the database […]."[3] Further, Marriott Guests have suffered an ascertainable loss in that they must undertake additional security measures, at their own expense, to minimize the risk of future data breaches including, without limitation, canceling credit cards used to reserve rooms with Marriott, updating the password and security measures on their Marriott rewards account, and canceling and renewing their passports to obtain new passport numbers. However, due to Marriott's ongoing and incomplete investigation, Marriott Guests have no guarantee that the above security measures will in fact adequately protect their personal information. As such, Plaintiffs and other Class Members have an ongoing interest in ensuring that their personal information is

[2] *Id.*

[3] *Id.*

protected from past and future cybersecurity threats.

THE PARTIES

5. Plaintiff Cynthia Husebo ("Plaintiff Husebo") is a citizen of the state of California, residing in Chino, California. Plaintiff has been a Marriott Guest since at least 2014, specifically a member of Marriott's rewards program, and provided Defendants with PII including her name, Marriott account password, email address, telephone number, date of birth, home and billing addresses, and credit card information.

6. As of the date of filing of this complaint, Plaintiff Husebo has not been notified by Marriott regarding the data breach but plans to obtain a copy of her credit report and further secure her PII after learning of the breach through public news sources. Plaintiff Husebo is informed and believes that her PII was compromised as a result of the 2014 Data Breach because her PII is located within Marriott's Starwood guest database. However, Plaintiff Husebo never received a notification from Marriott regarding the Data Breach or that her account information and PII was compromised as a result of the breach.

7. Plaintiff Matthew Tidd ("Plaintiff Tidd") is a citizen of the state of California, residing in Vacaville, California. Plaintiff has been a Marriott Guest since at least 2014, specifically a Starwood Preferred Guest, and provided Defendants with PII including, without limitation, his name, Marriott account password, email address, telephone number, date of birth, home and billing addresses, reservation history, and credit card information.

8. As of the date of filing of this complaint, Plaintiff Tidd received an email from Marriott informing him of the data breach and that his PII may have been compromised as a result of the breach.

9. Defendant Marriott International, Inc., and its subsidiary Marriott Hotel Services, Inc., ("Marriott") is a corporation organized and in existence under the laws of the State of Delaware and registered to do business in the State

of California. Marriott's Corporate Headquarters are located at 10400 Fernwood Road, Bethesda, Maryland 20817.

10. At all relevant times, Defendants were and are engaged in the business of owning and operating hotels and other resort properties in San Bernardino County and throughout the United States of America.

JURISDICTION

11. This is a class action.

12. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1331 because this action arises under the Constitution or laws of the United States and the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) and (6), in that, as to each Class defined herein:

(a) the matter in controversy exceeds $5,000,000.00, exclusive of interest and costs;

(b) this is a class action involving 100 or more class members; and

(c) this is a class action in which at least one member of the Plaintiff's class is a citizen of a State different from at least one Defendants.

13. The Court has personal jurisdiction over Defendants, which have at least minimum contacts with the State of California because they have conducted business there and have availed themselves of California's markets through their hotel and similar resort properties.

VENUE

14. Marriott, through its hotel ownership and management, has established sufficient contacts in this district such that personal jurisdiction is appropriate. Defendant is deemed to reside in this district pursuant to 28 U.S.C. § 1391(a).

15. In addition, Defendants have conducted business in this district, and has availed itself of California's markets through its marketing, ownership, and operations of hotel and similar properties. Venue is proper in this Court pursuant

to 28 U.S.C. § 1391(a).

FACTUAL ALLEGATIONS

16. "Marriott International, Inc. is a leading global lodging company with more than 6,700 properties across 130 countries and territories, reporting revenues of more than $22 billion in fiscal year 2017."[4] Marriott owns, manages, and operates hotel and other similar properties in California, and throughout the United States. Marriott requires its Guests to provide personally identifiable information ("PII") upon making a reservation via Defendants' website, reservation phone line, or mobile phone application and Guests expect Defendants to maintain strict confidentiality of the PII in Marriott's possession. Throughout the course of its business, Marriott has collected and maintained an extensive amount of its Guests' personal information including, without limitation, Guests' names, email addresses, home and billing addresses, telephone numbers, dates of birth, credit card numbers, passport numbers, and reservation history. Marriott Guests provide this personal information to Marriott in reliance on Defendants' assurances as to the protection and security of its Guests' PII.

17. However, on information and belief, Defendants failed, and continues to fail, to provide adequate protection of its Guests' personal and confidential information and has egregiously failed to provide sufficient and timely notice or warning of potential and actual cybersecurity breaches to its Guests.

18. At all relevant times, Marriott has made several assurances to its Guests that its Guests' privacy and security is of utmost importance to Marriott, and its Guests have relied on those assurances in providing Marriott with their PII. In fact, Marriott's Privacy Statement represents to its Guests that Marriott

[4] https://www.marriott.com/marriott/aboutmarriott.mi.

"values you as our guest and recognizes that privacy is important to you" and "We seek to use reasonable organizational, technical and administrative measures to protect Personal Data. "[5] Clearly, Marriott has failed to provide the security consistently promised to its Guests.

19. The types of information compromised in the 2014 Data Breach are highly valuable to identity thieves. The names, email addresses, recovery email accounts, telephone numbers, dates of birth, passwords, security question answers, credit card numbers, passport numbers, and other valuable PII can all be used to gain access to a variety of existing accounts and websites.

20. Despite these assurances, Marriott recently revealed that its Guests' personal information was subject to a massive data security breach that has been ongoing since 2014 affecting approximately 500 million Marriott Guests. Marriott released a statement on November 30, 2018, publicly informing Guests of the 2014 Data Breach for the first time. According to the statement, "[o]n September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database."[6] Further, "[f]or approximately 327 million of these guests, the information [stolen] includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates." To date, Marriott states that it "began sending emails on a rolling basis … to affected guests whose email addresses are in the Starwood guest reservation database" but no other actions have been taken. Moreover, no details have been released regarding how

[5] https://www.marriott.com/about/privacy.mi.

[6] "Starwood Guest Reservation Database Security Incident," available at https://answers.kroll.com/ (last visited December 3, 2018).

the Guests' information became compromised and whether steps have been taken to secure the information.

21. As a result of Defendants' failure to maintain adequate security measures and timely security breach notifications, Marriott Guests' personal and private information has been compromised and remains vulnerable. In fact, according to Marriott, they have "not finished identifying duplicate information in the database […]." Further, Marriott Guests have suffered an ascertainable loss in that they must undertake additional security measures, some at their own expense, to minimize the risk of future data breaches including, without limitation, canceling credit cards used to make numerous reservations over the last four years and changing the password and account information for their Marriott rewards account. However, due to Marriott's ongoing and incomplete investigation, Marriott Guests have no guarantee that the above security measures will in fact adequately protect their personal information. As such, Plaintiffs and other Class Members have an ongoing interest in ensuring that their personal information is protected from past and future cybersecurity threats.

22. The insufficient security policies and procedures implemented by Defendants are a material fact that a reasonable consumer would consider when deciding whether to create an account and provide Defendants with personal and confidential information. Had Plaintiffs and other Class Members known that Defendants failed to employ necessary and adequate protection of their personal information, they would not have created a Marriott rewards account, made a reservation through Marriott, or limited the PII shared with Marriott.

CLASS ACTION ALLEGATIONS

23. Plaintiffs bring this lawsuit as a class action on behalf of themselves and all others similarly situated as members of the proposed Class pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4). This action satisfies the numerosity, commonality, typicality, adequacy,

predominance, and superiority requirements of those provisions.

24. The Class is defined as:

> **Nationwide Class**: All individuals residing in the United States who made a reservation at a Marriott owned or operated hotel, or similar property, at any time, from four years prior to the filing of this complaint to the time of class certification, and whose personal or financial information was accessed, compromised, or stolen in the 2014 Data Breach (the "Nationwide Class" or "Class").
>
> **California Sub-Class:** All members of the Nationwide Class who made a reservation at a Marriott owned or operated hotel and reside in the State of California.

25. Collectively, the Nationwide Class and the California Sub-Class, and their class members, will be referred to herein as the "Class" and "Class Members," except where otherwise noted.

26. Excluded from the Class are: (1) Defendant, any entity or division in which Defendant has a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; (3) any Judge sitting in the presiding state and/or federal court system who may hear an appeal of any judgment entered; and (4) those persons who have suffered personal injuries as a result of the facts alleged herein. Plaintiffs reserve the right to amend the Class and Sub-Class definition if discovery and further investigation reveal that the Class should be expanded or otherwise modified.

27. Numerosity: Although the exact number of Class Members is uncertain and can only be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable. The disposition of the claims of these Class Members in a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Defendant's possession, custody, or control.

28. Typicality: Plaintiffs' claims are typical of the claims of the Class in that Plaintiff, like all Class Members, have made a reservation and provided Marriott with their PII throughout the duration of the class period. The representative Plaintiffs, like all Class Members, have been damaged by Defendants' misconduct in that they have had to undertake additional security measures, at their own time and expense, to minimize the risk of future data breaches. Furthermore, the factual bases of Defendants' misconduct are common to all Class Members and represent a common thread resulting in injury to all Class Members.

29. Commonality: There are numerous questions of law and fact common to Plaintiffs and the Class that predominate over any question affecting only individual Class Members. These common legal and factual issues include the following:

(a) Whether Defendants owed a duty of care to Plaintiffs and Class Members with respect to the security of their personal information;

(b) Whether Defendants had a legal and/or contractual duty to use reasonable security measures to protect Plaintiffs' and Class Members' personal information;

(c) Whether Defendants took reasonable steps and measures to safeguard Plaintiffs' and Class Members' personal information;

(d) Whether Defendants breached their duty to exercise reasonable care in handling Plaintiffs' and Class Members' personal information;

(e) Whether Defendants' acts and omissions described herein give rise to claims of negligence and/or deceit by concealment;

(f) Whether Defendants' security procedures and practices violated *California Business & Professions Code* §§ 17200 *et seq.*;

(g) Whether Defendants' security procedures and practices violated *California Civil Code* §§ 1798.90 *et seq.;*

(h) Whether Defendants knew or should have known of the 2014 Data Breach and when they knew or should have known;

(i) Whether Defendants had a duty to promptly notify Class Members that their personal information was, or potentially could be, compromised; and

(j) Whether Plaintiffs and other Class Members are entitled to damages or equitable relief, including but not limited to, a preliminary and/or permanent injunction.

30. Adequate Representation: Plaintiffs will fairly and adequately protect the interests of the Class Members. Plaintiffs have retained attorneys experienced in the prosecution of complex class actions, including consumer and product defect class actions, and Plaintiffs intend to prosecute this action vigorously.

31. Predominance and Superiority: Plaintiffs and Class Members have all suffered and will continue to suffer harm and damages as a result of Defendants' unlawful and wrongful conduct. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Absent a class action, most Class Members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Because of the relatively small size of the individual Class Members' claims, it is likely that only a few Class Members could afford to seek legal redress for Defendants' misconduct. Absent a class action, Class Members will continue to incur damages, and Defendants' misconduct will continue without remedy. Class treatment of common questions of law and fact would also be a superior method to multiple individual actions or piecemeal litigation in that class treatment will conserve the resources of the courts and the litigants and will promote consistency and efficiency of adjudication.

FIRST CAUSE OF ACTION

(Violation of California Business & Professions Code § 17200, *et seq*.)

32. Plaintiffs incorporate by reference the allegations contained in each and every paragraph of this Complaint.

33. Plaintiffs bring this cause of action on behalf of himself and on behalf of the Nationwide Class, or in the alternative, on behalf of the California Sub-Class.

34. As a result of their reliance on Defendants' representations and omissions, Marriott Guests' utilizing its hotel reservation services suffered an ascertainable loss due to Defendants' failure to provide adequate protection of its Marriott Guests' personal and confidential information and failure to provide sufficient and timely notice or warning of potential and actual cybersecurity breaches.

35. California Business & Professions Code § 17200 prohibits acts of "unfair competition," including any "unlawful, unfair or fraudulent business act or practice" and "unfair, deceptive, untrue or misleading advertising."

36. Plaintiffs and Class Members are reasonable consumers who expected Defendants to vehemently protect the personal information entrusted to them and to be informed by Defendants of potential and actual cybersecurity vulnerabilities as soon as Defendants became aware of such threat.

37. Defendants' acts and omissions were intended to induce Plaintiffs and Class Members' reliance on Defendants' explicit and implied guarantee that their personal information was secure and protected, to increase the number of Marriott Guests, and, ultimately, to increase Defendant's revenues. Plaintiffs and the Class Members were deceived by Defendants' failure to properly implement adequate, commercially reasonable security measures to protect their personal information, and Defendants' failure to promptly notify them of the security breach. As a result, Defendants' conduct constitutes "fraudulent" business acts

or practices.

38. Defendants' conduct was and is likely to deceive consumers.

39. In failing to implement adequate security procedures and protocols to protect Plaintiffs and Class Members' personal information and promptly notify Plaintiffs and Class Members of potential and actual security threats, Defendants have knowingly and intentionally concealed material facts and breached its duty not to do so.

40. Defendants were under a duty to Plaintiffs and Class Members to protect Marriott Guests' personal information and promptly notify Marriott Guests of potential and actual security threats, and other omitted facts alleged herein, because:

(a) Defendants were in a superior position to know the specifics of a potential or actual security breach; and

(b) Defendants actively concealed information known to it regarding potential and actual security breaches affecting Marriott Guests' account information.

41. The facts Defendants concealed from or did not disclose to Plaintiffs and Class Members are material in that a reasonable person would have considered them to be important in deciding whether to utilize Defendants' hotel reservation services or cancel, change or otherwise modify their account information. Had Plaintiffs and other Class Members known that Defendants failed to employ necessary and adequate protection of their personal information and would fail to timely notify them of potential security breaches, they would not have created a Marriott Guest account, made a hotel reservation through Marriott, or would not have provided PII to Marriott.

42. By their conduct, Defendants have engaged in unfair competition and unlawful, unfair and fraudulent business practices. Defendants' unfair or deceptive acts or practices occurred repeatedly in Defendants' trade or business

and were capable of deceiving a substantial portion of the purchasing public.

43. As a direct and proximate result of Defendants' unlawful, unfair and deceptive practices, Plaintiffs and Class Members will continue to suffer actual damages.

44. Defendants have been unjustly enriched and should be required to make restitution to Plaintiffs and Class Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code.

SECOND CAUSE OF ACTION

(Violation of the California Customer Records Act, California Civil Code § 1798.80, *et seq*.)

45. Plaintiffs incorporate by reference the allegations contained in each and every paragraph of this Complaint.

46. Plaintiffs bring this cause of action on behalf of themselves and on behalf of the California Sub-Class.

47. The California Legislature enacted Civil Code § 1798.81.5 "to ensure that personal information about California residents is protected." The statute requires that any business that "owns, licenses, or maintains personal information about a California resident … implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

48. Defendants are "business(es)" as defined by Civil Code § 1798.80(a).

49. Plaintiffs and California Sub-Class Members are "individual[s]" as defined by Civil Code § 1798.80(d).

50. The personal information taken in the data breach was "personal information" as defined by Civil Code § 1798.80(e) and 1798.81.5(d), which includes "information that identifies, relates to, describes, or is capable of being

associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."

51. The breach of the personal information of an estimated 500 million Marriott Guests was a "breach of the security system" of Defendants as defined by Civil Code § 1798.82(g).

52. By failing to implement reasonable security measures appropriate to the nature of the personal information of Marriott Guests, Defendants violated Civil Code § 1798.81.5.

53. In addition, by failing to immediately notify all affected Marriott Guests that their personal information had been acquired or may have been acquired by unauthorized persons in the data breach, Defendants violated Civil Code § 1798.82. Defendants' failure to immediately notify Marriott Guests of the breach caused Class Members to suffer damages because they have lost the opportunity to immediately: (i) buy identity protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service; (iii) purchase or otherwise obtain credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services; (v) place and renew credit fraud alerts on a quarterly basis; (vi) routinely monitor public records, loan data, or criminal records; (vii) contest fraudulent charges and other forms of criminal, financial and medical identity theft, and repair damage to

credit and other financial accounts; and (viii) take other steps to protect themselves and recover from identity theft and fraud.

54. Because they violated Civil Code § 1798.81.5 and 1798.82, Defendants "may be enjoined" under Civil Code § 1798.84(e).

55. Plaintiffs request that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures to protect its Guests' personal information, including, but not limited to, ordering that Defendants:

(a) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

(b) engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices;

(c) audit, test, and train its security personnel regarding any new or modified procedures;

(d) purge, delete and destroy, in a secure manner, Marriott Guests data not necessary for its business operations;

(e) conduct regular database scanning and securing checks consistent with prudent industry practices;

(f) periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices;

(g) receive periodic compliance audits by a third party regarding the security of the computer systems, cloud-based services, and application software Defendants use to store the personal information of current and former Marriott Guests;

(h) meaningfully educate its current and former Marriott Guests about

the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves; and

(i) provide ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and Class Members.

56. As a result of Defendants' violation of Cal. Civ. Code § 1798.81.5, Plaintiffs and Class Members have incurred and will incur damages, including but not necessarily limited to: (1) the loss of the opportunity to control how their personal information is used; (2) the diminution in the value and/or use of their personal information entrusted to Defendants for the purpose of deriving services from Defendants and with the understanding that Defendants would safeguard their personal information against theft and not allow access and misuse of their personal information by others; (3) the compromise, publication, and/or theft of their personal information; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised personal information to open new financial and/or health care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their personal information , which remain in Defendants' possession and are subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information

in their possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the personal information compromised as a result of the data breach for the remainder of the lives of the Class Members.

57. Plaintiffs seek all remedies available under Civil Code § 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including California Code of Civil Procedure § 1021.5.

THIRD CAUSE OF ACTION

(Negligence)

58. Plaintiffs incorporate by reference the allegations contained in each and every paragraph of this Complaint.

59. Plaintiffs bring this cause of action on behalf of themselves and on behalf of the Nationwide Class.

60. Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their personal information in their possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, implementing, maintaining and testing Defendants' security systems and protocols, consistent with industry standards and requirements, to ensure that Plaintiffs' and Class Members' personal information in Defendants' possession was adequately secured and protected. Defendants further owed a duty to Plaintiffs and Class Members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

61. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate security

practices. Defendants solicited, gathered, and stored the personal data provided by Plaintiffs and Class Members in the regular course of its business. Defendants knew that a breach of its systems would cause damages to Plaintiffs and Class Members, and Defendants had a duty to adequately protect such sensitive personal information.

62. Similarly, Defendants owed a duty to Plaintiffs and Class Members to timely disclose any incidents of data breaches, where such breaches compromised the personal information of Plaintiffs and Class Members. Plaintiffs and Class Members were foreseeable and probable victims of any inadequate notice practices. Defendants knew that, through its actions and omissions, it had caused the sensitive personal information of Plaintiffs and Class Members to be compromised and accessed by unauthorized third parties yet failed to mitigate potential harm to Marriott Guests by providing timely notice of the security breach.

63. Defendants breached the duties owed to Plaintiffs and Class Members by failing to exercise reasonable care in the adoption, implementation, and maintenance of adequate security procedures and protocols and by failing to timely notify Plaintiffs and Class Members of potential and actual security breaches. Defendants' breach of the duties owed to Plaintiffs and Class Members caused injuries to Plaintiffs and Class Members, including but not limited to a) theft of their personal information; b) costs associated with the detection and prevention of identity theft; c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the aforementioned data breaches, including without limitation finding fraudulent charges, cancelling and reissuing credit cards and bank accounts, purchasing credit monitoring and identity theft protection, and the stress, nuisance and annoyance of dealing with all issues resulting from the data breaches; d) the imminent and impending injury

flowing from potential fraud and identity theft posed by the unauthorized control and use of their personal information by third parties; e) damages to and diminution in value of their personal information entrusted to Defendants with the understanding that Defendants would safeguard their data against theft and not allow access and misuse of their data by others; and f) the continued risk to their personal information, which remains in Defendants' possession and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect data in their possession.

64. But for Defendants' negligent and wrongful breach of the duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been harmed and could have taken remedial measures to protect their personal information.

65. Plaintiffs and Class Members are entitled to and seek actual damages and reasonable attorneys' fees and costs.

FOURTH CAUSE OF ACTION

(Deceit by Concealment, Cal. Civ. Code §§ 1709, 1710)

66. Plaintiffs incorporate by reference the allegations contained in each and every paragraph of this Complaint.

67. Plaintiffs bring this cause of action on behalf of themselves and on behalf of the California Sub-Class.

68. Defendants had an obligation to disclose to all class members that their Marriott reservation information and PII were an easy target for hackers and Defendants had not implemented measures to protect them.

69. Defendants did not do these things. Instead, Defendants willfully deceived Plaintiffs and the Class by concealing the true facts concerning their data security, which Defendants were obligated to, and had a duty to, disclose. Additionally, Marriott made numerous representations to ensure users that their PII and other data was safe, and Marriott was dedicated to maintaining that

security.

70. Had Defendants disclosed the true facts about its poor data security, Plaintiffs and the Class would have taken measures to protect themselves. Plaintiffs and the Class justifiably relied on Defendants to provide accurate and complete information about Defendants' data security, and Defendants did not.

71. Alternatively, given the security holes in Defendants' services and Defendant's failure to detect those holes, much less fix them, Defendants simply should have shut down their current service. Independent of any representations made by Defendants, Plaintiffs and the Class justifiably relied on Defendants to provide a service with at least minimally adequate security measures and justifiably relied on Defendants to disclose facts undermining that reliance.

72. Rather than disclosing to Plaintiff and the Class that its services were unsafe and users' PII was exposed to theft on a grand scale, Defendants continued on and concealed any information relating to the inadequacy of their security.

73. These actions are "deceit" under Cal. Civil Code § 1710 in that they are the suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.

74. As a result of this deceit by Defendants, it is liable under Cal. Civil Code § 1709 for "any damage which [Plaintiff and the Class] thereby suffer []."

75. As a result of this deceit by Defendants, the PII of Plaintiffs and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiffs and Class Members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other

expenses relating to identity theft losses or protective measures.

76. Defendants' deceit as alleged herein is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants conducted with the intent on the part of Defendants of depriving Plaintiffs and the Class of "legal rights or otherwise causing injury." As a result, Plaintiffs and the Class are entitled to punitive damages against Defendants under Civil Code § 3294(a).

RELIEF REQUESTED

77. Plaintiffs, on behalf of themselves, and all others similarly situated, requests the Court enter judgment against Defendants, as follows:

(a) An order certifying the proposed Class, designating Plaintiffs as named representatives of the Class, and designating the undersigned as Class Counsel;

(a) An order enjoining Defendants from further unfair and deceptive business practices regarding the maintenance and protection of Marriott Guests' personal information;

(b) An award to Plaintiffs and the Class for compensatory, exemplary, and statutory damages, including interest, in an amount to be proven at trial;

(c) A declaration that Defendants must disgorge, for the benefit of the Class, all or part of the ill-gotten revenues they collected from their conduct alleged herein, or make full restitution to Plaintiffs and Class Members;

(d) An award of attorneys' fees and costs, as allowed by law;

(e) An award of attorneys' fees and costs pursuant to California Code of Civil Procedure § 1021.5;

(f) An award of pre-judgment and post-judgment interest, as provided by law; and

(g) Such other relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

78. Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable.

Dated: December 3, 2018

Respectfully submitted,

Capstone Law APC

By: /s/ Tarek Zohdy
Tarek H. Zohdy
Cody R. Padgett
Trisha K. Monesi

Attorneys for Plaintiffs